UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/507,190	09/09/2004	Pim Theo Tuyls	NL 020192	1803

24737 7590 03/02/2007

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
TRAORE, FATOUMATA	
ART UNIT	PAPER NUMBER
2109	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/02/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/507,190	TUYLS ET AL.	
	Examiner	Art Unit	
	Fatoumata Traore	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 September 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 September 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response of the preliminary amendment filing of September 9, 2004. Claims 1-19 are pending and have been considered below.

Claim Objections

2. Claims 16-19 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Claims 16-18 are system/device claims, which refer back to Claims 1, 16, 17. The Office considers any claim that refers to another claim as dependent thereon, i.e. a dependent claim. Since Claim 1 is a method claim comprising several steps and Claims 16-18 fail to add, delete, or change any of these steps, Claims 16-18 fail to further limit it parent claims. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-19 are rejected under 35 U.S.C. 101 because: Claims to processes that do nothing more than solve mathematical problems manipulate abstract ideas or concepts are complex to analyze and are addressed herein.

If the "acts" of a claimed process manipulate only numbers, abstract concepts or ideas, or signals representing any of the foregoing, the acts are not being applied

to appropriate subject matter. Gottschalk v. Benson, 409 U.S. 63, 71 - 72, 175 USPQ 673, 676 (1972). Thus, a process consisting solely of mathematical operations, i.e. converting one set of numbers into another set of numbers, does not manipulate appropriate subject matter and thus cannot constitute a statutory process. In practical terms, claims define nonstatutory processes if they:

– consist solely of mathematical operations without some claimed practical application (i.e., executing a "mathematical algorithm"); or

– simply manipulate abstract ideas, e.g., a bid (Schrader, 22 F.3d at 293-94, 3 USPQ2d at 1458-59) or a bubble hierarchy (Warmerdam, 33 F.3d at 1360, 31 USPQ2d at 1759), without some claimed practical application. Cf. Alappat, 33 F.3d at 1543 n.19, 31 USPQ2d at 1556 n.19 in which the Federal Circuit recognized the confusion:

The Supreme Court has not been clear . . . as to whether such subject matter is excluded from the scope of 101 because it represents laws of nature, natural phenomena, or abstract ideas. See Diehr, 450 U.S. at 186 (viewed mathematical algorithm as a law of nature); Gottschalk v. Benson, 409 U.S. 63, 71-72 (1972) (treated mathematical algorithm as an "idea"). The Supreme Court also has not been clear as to exactly what kind of mathematical subject matter may not be patented. The Supreme Court has used, among others, the terms "mathematical algorithm," "mathematical formula," and "mathematical equation" to describe types of mathematical subject matter not entitled to patent protection standing alone. The Supreme Court has not set forth, however, any consistent or clear

explanation of what it intended by such terms or how these terms are related, if at all. Certain mathematical algorithms have been held to be nonstatutory because they represent a mathematical definition of a law of nature or a natural phenomenon. For example, a mathematical algorithm representing the formula E = mc2 is a "law of nature" — it defines a "fundamental scientific truth" (i.e., the relationship between energy and mass). To comprehend how the law of nature relates to any object, one invariably has to perform certain steps (e.g., multiplying a number representing the mass of an object by the square of a number representing the speed of light). In such a case, a claimed process which consists solely of the steps that one must follow to solve the mathematical representation of E = mc2 is indistinguishable from the law of nature and would "preempt" the law of nature. A patent cannot be granted on such a process.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-4, 6, 9-12, 16, 17, 19 are rejected under 35 U.S.C. 102(b) as being anticipated by **Matyas et al** (US 5953420).

Claims 1, 16, 17, 19: **Matyas et al** discloses a method for establishing an authenticated shared secret value between a pair of users comprising:

a first party and a second party, in which the first party holds a value p1 and a symmetrical polynomial P(x, y) fixed in the first argument by the value p1(User A generate a secret value X1a, preferably 2^159 > X<= q-2, then generates a public value Y1a from the secret value X1) (column 6, lines 15-25), and the first party performs the steps of sending the value p1 to the second party (Each party transmits its own public value to the over party) (column 6, lines 35-40) , receiving a value p 2 from the second party and calculating the common secret S1 by evaluating the polynomial P(p 1, y) in p2 (each party generates a value Z1 from the public value Y1 received from the other party and its own secret value X1 as Z1 =Y1^x1 mod p) (column 6, lines 44-50), characterized in that the first party additionally holds a value 1 and a symmetrical polynomial Q(x, z) fixed in the first argument by the value q1(User A generates a secret value X2a, then generates a public value Y2 from the secret value X2) (column 7, lines 5-15), and further performs the steps of sending q1 to the second party, receiving a value q.2 from the second party and calculating the secret S 1 as S1=Q(q.1, q 2). P(p. 1, p 2) (each party transmit its own public value Y2 to the other party then generates a value Z2 from the public value Y2 received from the other party and its own secret value X2 as Z2 = Y2^x2 mod p) (column 7, lines 25-40).

Claim 2: **Matyas et al** discloses a method for establishing an authenticated shared secret value between a pair of users as in claim 1 above, and further discloses that the first party further performs the steps of obtaining a random

number r1 (user A generates a secret value X1a using a pseudorandom number generator) (column 6, lines 15-20), calculating r1. q1 (generates a public value Y1 from the secret value X1 as Y1 = G^x1 mod p) (column 6 lines 20-25), sending r1.q1 to the second party(each party transmits its own public value Y1 to the other party) (column 6, lines 35-38), receiving r2.q2 from the second party and calculating the secret S1 as S1=Q(q1, r1.r2.q2).P (p1, p2) (each party generates a value Z2 from the public value Y2 received from the other party and its own secret value X2 as Z2 =Y2^x2 mod p) (column 7, lines 33-45).

Claim 3: **Matyas et al** discloses a method for establishing an authenticated shared secret value between a pair of users as in claim 2 above, and further discloses that the first party holds the value q1 multiplied by an arbitrarily chosen value r (user A generates a secret value X1a using a pseudorandom number generator) (column 6, lines 15-20), and the product Q (q1, z). P (p1, y) instead of the individual polynomials P (p1, y) and Q (q1, z) (generates a public value Y1 from the secret value X1 as Y1 = G^x1 mod p) (column 6 lines 20-25), and the first party performs the steps of calculating r1.r.q1, sending r1.r.q1 to the second party, receiving r2.r.q2 from the second party and calculating the secret S1 as S1= Q(q1, r1.r2.r.q2).P(p1, p2) (each party generates a value Z2 from the public value Y2 received from the other party and its own secret value X2 as Z2 =Y2^x2 mod p) (column 7, lines 33-45).

Claim 4: **Matyas et al** discloses a method for establishing an authenticated shared secret value between a pair of users as in claim 1 above, and further discloses that the second party holds a value p2 and a value q2(User B generates a secret value X2b, then generates a public value Y2 from the secret value X2) (column 7, lines 6-15), the symmetrical polynomial P (x, y) fixed in the first argument by the value p2 (User B generates a secret value X2b, then generates a public value Y2 from the secret value X2) (column 7, lines 6-15), the symmetrical polynomial Q(x, z) fixed in the first argument by the value q2 (User B generates a secret value X2b, then generates a public value Y2 from the secret value X2) (column 7, lines 6-15), and the second party performs the steps of sending q2 to the first party, receiving q1 from the first party and calculating a secret S2 as S2=Q(q2, q1).P>(p2, p1)whereby the common secret has been generated if the secret S2 = S1Each user transmits its own public value Y to the other user, then generates , from its own secret value X and the public Y transmitted to it from the other user a common shared secret value Z as Z = g^(xa.xb) mod p which is generated by each user as Z a =Yb^xa mod p Zb = Ya^b mod p respectively it is shown that equations Z = Y^x mod p and Zb = Ya^xb mod are equivalent and all yield the same value, that is Za= Zb= Z) (column 3, lines 40-8 and column 4, lines 1-5).

Claim 9: **Matyas et al** discloses a method for establishing an authenticated shared secret value between a pair of users as in claim 1above, and further

discloses that the first party and the second party use a non-linear function on the generated secret S1 and S2, respectively, before using it as a secret key in further communications (finally each party generates a value Z1 from the public value Y1 received from the other party and its own secret value X1 as Z1 =Y1^x1 mod p, Z2 = Y2^x2 mod p) (column 6, lines 44-50 and column 7, lines 34-50).

Claim 10: **Matyas et al** discloses a method for establishing an authenticated shared secret value between a pair of users as in claim 9 above, and further discloses that the a one-way hash function is applied to the generated secrets S1 and S2 (the concatenated value is passes through a one way hash function to generate a hash value) (column 5, lines25-30).

Claim 11: **Matyas et al** discloses a method for establishing an authenticated shared secret value between a pair of users as in claim 9 above, and further discloses that the a a non-linear function in the form of a polynomial is applied to the generated secrets S1 and S2 (finally each party generates a value Z1 from the public value Y1 received from the other party and its own secret value X1 as Z1 =Y1^x1 mod p, Z2 = Y2^x2 mod p) (column 6, lines 44-50 and column 7, lines 34-50).

Claim 12: **Matyas et al** discloses a method for establishing an authenticated shared secret value between a pair of users as in claim 1 above, and further

discloses a step of verifying that the second party knows the secret S1 (the Z1 value generated by the two parties should be equal) (column 6, lines60-65).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 5-8, 13-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Matyas et al** (US 5953420) in view of **Menezes et al** (handbook of Applied Cryptography, ISBN 0-8493-8523-7 1997).

Claim 5: **Matyas et al** discloses a method for establishing an authenticated shared secret value between a pair of users as in claim 1 above, but does not explicitly discloses that a trusted third party performs the steps of choosing a symmetric (n+1).(n+1) matrix T, constructing the polynomial P using entries from the matrix T as respective coefficients of the polynomial P. However **Menezes et al** discloses a method of implementing a common secret generation and further discloses, that a trusted third party performs the steps of choosing a symmetric (n+1).(n+1) matrix T(A trusted party T creates a random secret k x k symmetric Matrix D over Fq (page 506, section 12.35), constructing the polynomial P using entries from the matrix T as respective coefficients of the polynomial P(T gives to each user Ui the secret key Si, defined as row I of the n.k matrix S = (DG)^T.(Si

is a k-tuple over Fq of k.lg(q) bits, allowing Ui to compute any entry in row I of (D.G)^T G)(page 505, section 12.35) constructing the polynomial Q(x, y), choosing the value p1, the value p2 the value q1 and the value q2, sending the value p1, the value q1, the polynomial P(x, y) fixed in the first argument by the value p1 and the polynomial Q(x, z) fixed in the first argument by the value q1 to the first party, and sending the value p2, the value q 2, the polynomial P(x, y) fixed in the first argument by the value p2 and the polynomial Q(x, z) fixed in the first argument by the value q2 to the second party (Users Ui and Uj compute the common secret Ki,j = Kj,I of bit length m = lg(q) as follows. Using Si and column j of G.Ui computes the (I, j) entry of the n.n symmetric matrix K = (DG)^TG. Using Sj and column I of G.Uj similarly computes the (j, I) entry which is equal to the (I, j) entry since K is symmetric) (page 506, section 12.35). Therefore, it would have been obvious to one having ordinary skills in the art at the time the invention was made for **Matyas et al** to use Blom's symmetric key pre-distribution mechanism. One would have been motivated to do so in order to provide unconditional security.

Claim 6: **Matyas et al** and **Menezes et al** disclose a method for establishing an authenticated shared secret value between a pair of users as in claim 5 above, and **Matyas et al** further discloses that the trusted third party further arbitrarily chooses a value r user A generates a secret value X1a using a pseudorandom number generator (column 6, lines 15-20), sends the value r1 instead of the

value q1 and the product Q(q1, z)P(p 1, y) instead of the individual polynomials P(p1, y) and Q(q1, z) to the first party (generates a public value Y1 from the secret value X1 as Y1 = G^x1 mod p) (column 6 lines 20-25) and sends the value r. q2 instead of the value q.2 and the product Q(q2, z)P(p2, y) instead of the individual polynomials P(p2, y) and Q(q2, z) to the second party(each party generates a value Z2 from the public value Y2 received from the other party and its own secret value X2 as Z2 =Y2^x2 mod p) (column 7, lines 33-45). Therefore, it would have been obvious to one having ordinary skills in the art at the time the invention was made for **Matyas et al** to let a trusted third party choose an arbitrarily value r. One would have been motivated to do so in order to assure the authenticity of the generated keys.

Claim 7: **Matyas et al** and **Menezes et al** disclose a method for establishing an authenticated shared secret value between a pair of users as in claim 5 above, and **Menezes et al** further discloses that the trusted third party further performs the steps of choosing a set comprising m values p1(as described below, a trusted communications channel is used to exchange the static public key values that are used to assure the authenticity of the keys that are generated in accordance with the present invention) (column 4, lines 44- 50) including the values p1 and p2, calculating a space A from the tensor products Pi^V XOR Pj^v of the Vandermonde vectors Pi^v built from the set of values pi, choosing a vector ŷ1 and a vector ŷ2 from the perpendicular space A of the space A (A

trusted party T creates a random secret k x k symmetric Matrix D over Fq (page 506, section 12.35) , ΓŷT., constructing a matrix TΓ1 = T+Γ1 from the vector Y1 and a matixTV2 = T+Γ2 from the vector Y2, constructing a polynomial P^Γ1(x, y) fixed in the first argument by the value p1 to the first party using entries from the matrix T.sub..GAMMA..sub..sub.1,and sending the polynomial P.sup..GAMMA..sup..sub.1(x,y) fixed in the first argument by the value p.sub.1 to the first party (T gives to each user Ui the secret key Si, defined as row I of the n.k matrix S = (DG)^T.(Si is a k-tuple over Fq of k.lg(q) bits, allowing Ui to compute any entry in row I of (D.G)^T G)(page 505, section 12.35), and constructing a polynomial P.sup..GAMMA..sup..sub.2(x,y) using entries from the matrix T.sub..GAMMA..sub..sub.2 and sending the polynomial P.sup..GAMMA..sup..sub.2(x,y) fixed in the first argument by the value p.sub.2 to the second party (Users Ui and Uj compute the common secret Ki,j = Kj,I of bit length m = lg(q) as follows. Using Si and column j of G.Ui computes the (I, j) entry of the n.n symmetric matrix K = (DG)^TG. Using Sj and column I of G.Uj similarly computes the (j, I) entry which is equal to the (I, j) entry since K is symmetric) (page 506, section 12.35). Therefore, it would have been obvious to one having ordinary skills in the art at the time the invention was made for **Matyas et al** to construct matrix and polynomial entries from matrix. One would have been motivated to do so in order to assure the authenticity of the generated keys.

Claim 8: **Matyas et al** and **Menezes et al** disclose a method for establishing an authenticated shared secret value between a pair of users as in claim 5 above, and **Menezes et al** further discloses that a number m' of values pi, and m'<m, are distributed to additional parties (each of n users is given initial secret keying and public data) (page 506, section 12.35). Therefore, it would have been obvious to one having ordinary skills in the art at the time the invention was made for **Matyas et al** to distributed initial keys to additional parties. One would have been motivated to do so in order to assure the authenticity of the generated keys.

Claim 13: **Matyas et al** and **Menezes et al** disclose a method for establishing an authenticated shared secret value between a pair of users as in claim 12 above, and **Menezes et al** further discloses that the first party subsequently applies a zero-knowledge protocol to verify that the second party knows the secret S1 (The prover claiming to be A selects a random element from pre-defined set as its secret commitment, and from this computes an associated (public) witness. This provides initial randomness for variation from other protocols runs, and essentially defines a set of questions all of which the prove claims to be able to answer, thereby a priori constraining her forthcoming response. By protocol design, only the legitimate party A, with knowledge of A's secret, is truly capable of answering all the questions, and the answer to any one of these provides no information about A's long-term secret) (pages 409-410, section (IV)). Therefore, it would have been obvious to one having ordinary skills in the art at the time the

invention was made for **Matyas et al** to use a zero-knowledge protocol. One would have been motivated to do so in order to provide unconditional security.

Claim 14: **Matyas et al** and **Menezes et al** disclose a method for establishing an authenticated shared secret value between a pair of users as in claim 12 above, and **Menezes et al** further discloses that the first party subsequently applies a commitment-based protocol to verify that the second party knows the secret S1 (The prover claiming to be A selects a random element from pre-defined set as its secret commitment, and from this computes an associated (public) witness. This provides initial randomness for variation from other protocols runs, and essentially defines a set of questions all of which the prove claims to be able to answer, thereby a priori constraining her forthcoming response. By protocol design, only the legitimate party A, with knowledge of A's secret, is truly capable of answering all the questions, and the answer to any one of these provides no information about A's long-term secret) (pages 409-410, section (IV)). Therefore, it would have been obvious to one having ordinary skills in the art at the time the invention was made for **Matyas et al** to use a commitment based protocol. One would have been motivated to do so in order to provide unconditional security.

Claim 15: **Matyas et al** and **Menezes et al** disclose a method for establishing an authenticated shared secret value between a pair of users as in claim 14 above, and **Menezes et al** further discloses that the second party uses a symmetric

cipher to encrypt a random challenge (b chooses a random r, computes the witness x = h(r) (x demonstrates knowledge of r without disclosing it and computes the challenge e = PA(r, B)) (page 404, section (I)), and sends the encrypted random challenge to the first party(B sends the encrypted random challenge to A. A decrypts e to recover r' and B' computes x' = h (r') (page 404, section (I) and the first party subsequently uses the same symmetric cipher as a commit function to commit himself to a decryption of the encrypted random challenge (A sends r= r' to B. B succeeds with unilateral entity authentication of A upon verifying) (page 404, section (I)). Therefore, it would have been obvious to one having ordinary skills in the art at the time the invention was made for **Matyas et al** to symmetric cipher. One would have been motivated to do so in order to preclude chosen text attacks (page 404, section (I)).

8. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Matyas et al** (US 5953420) in view of **Menezes et al** (handbook of Applied Cryptography, ISBN 0-8493-8523-7 1997) and in further view of **Oishi** (US 6298153).

Claim 18: **Matyas et al** and **Menezes et al** disclose a method for establishing an authenticated shared secret value between a pair of users as in claim 17 above. While neither reference explicitly discloses comprising storage means (303) for storing the polynomial P and the polynomial Q in the form their respective coefficients. However **Oishi** disclose a similar system, which further discloses a storage means (figure 3). Therefore, it would have been obvious to one having

ordinary skill in the art at the time the invention was made to use a storage means. One would have been motivated to do so in order to maintain data integrity.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Herzberg et al (US 5202921) Method and apparatus for authenticating users of a communication system to each other.

b. Chaum (US 4996711) Selected-exponent signature systems.

c. Matyas et al (US 5953420) Method and apparatus for establishing an authenticated shared secret value between a pair of users.

d. Oishi (US 6298153) Digital signature method and information communication system and apparatus using such method.

e. Dwork et al (US 5539826) method for message authentication from non-malleable crypto system.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:30 a.m. to 4:30 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jim W. Myhre, can be reached on (571) 272 6722. The fax phone number

for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 274-1685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT
February 27, 2007

James W. Myhre
Supervisory Patent Examiner